NATIONAL MARITIME SECURITY ADVISORY COMMITTEE (NMSAC)

Task Statement #T2021-03

Recommendations on Cybersecurity Information Sharing

Draft report to NMSAC by the T2021-03 Cybersecurity Information Sharing Sub-Committee

I. OVERVIEW

II. PROBLEM STATEMENT

The Coast Guard seeks industry input, via the National Maritime Security Advisory Committee (NMSAC), on ways to enhance cyber security information sharing between the Coast Guard and marine transportation system (MTS) stakeholders.

III. BACKGROUND

With the ever-evolving cyber threat, government agencies and MTS stakeholders must deliberately share information to protect the marine transportation system. This becomes especially critical and challenging based on the speed in which cyber threats originate, grow, and spread. Government agencies and MTS stakeholders are sharing cyber threat information through a number of coordinating bodies from the local to the international level.

IV. NMSAC SUB-COMMITTEE MEMBERS:

A. Chair

- Laurie Thomas, University of Findlay, Academic Community

B. Co-Chair

- Edward Madura, Port of Everett, Port Authorities

C. NMSAC Members

- James Fowler, Cooper T. Smith, Terminal Owners/Operators
- Jeffrey Musk, Sprague Operating Resources, Facility Owners/Operators
- Robert Matticola, NY Waterway Ferry, Vessel Owners/Operators
- April Danos, Stephenson Technologies Corporation, Maritime Industry
- Sean Kline, Chamber of Shipping of America, Maritime Industry

D. NON-NMSAC Members

- Michael Edgerton, Port of New York/New Jersey, Port Authority

E. Other Contributors

- Scott Dickerson, Executive Director, Maritime Transportation System Information Sharing Analysis Center (MTS-ISAC)
- Christy Coffey, VP of Operations, MTS-ISAC
- Deborah Kobza, Director Maritime Security Resilience Alliance, MPS-ISAO
- Peter Kaleda, Partner AliTek Response Solutions

V. DUE DATES

NMSAC should provide findings and recommendations at the public meeting in May 2022.

VI. COAST GUARD TECHNICAL REPRESENTATIVES

Mr. Ryan Owens
NMSAC Alternate Designated Federal Official
202-372-1108

LCDR Kelley Edwards
Office of Port & Facility Compliance
Critical Infrastructure Protection Branch

VII. INTRODUCTION

This report documents the work and results of the Cybersecurity Vulnerability Assessments of the National Maritime Security Advisory Committee (NMSAC). The work was based on Task Statement T2021_0 from the United States Coast Guard (USCG) to the Committee on October 28, 2021. This task was accepted by the NMSAC Committee on October 28, 2021, to address specific questions related to Tasking #T2021_03: Cybersecurity Information Sharing.

VIII. SUB-COMMITTEE TASK, SCOPE AND ACTIVITIES

This section should include a summary of the work conducted by the Sub-Committee to answer the tasking

A. Meetings Conducted by Sub-Committee:

- Information Sharing Subcommittee Meeting 01/19/2022
- Threat Intelligence Partnership for MTS Cybersecurity 02/15/2022
- MTS-ISAC, Briefing 04/20/2022
- MPS-ISAO, Briefing 04/20/2022

B. Sources Consulted by Sub-Committee:

- MTS-ISAC Overview NMSAC shared PowerPoint (April 2022)
- MTS-ISAC Possible Cybersecurity Controls for MARSEC Levels (April 2022)
- MPS-ISAO NMSAC Information Sharing RFI Response (April 2022)
- MPS-ISAO Security Briefing (April 2022)
- US DHS/CISA Cyber Storm VIII Exercise (March 2022) Local AMSC (Area Maritime Security Committee)
- USCG-CG-2 "Threat Intelligence Partnership for MTS Cybersecurity"

Local RIG (Reginal Intelligence Group)

State Fusion Center

IX. DESCRIPTION OF TASKS/DELIVERABLES

NMSAC is tasked with creating a working group to analyze and provide feedback on ways to enhance cyber information sharing between the government and MTS stakeholders, to include the following:

A. Provide industry perspectives on existing inefficiencies or gaps related to cyber information sharing.

- Information is in silos. If you are a member of the MTS-ISAC or MPS-ISAO you are sharing within that community, but there is no cross sharing between the two and both have MTS partners as customers. There is also a concern that membership in the ISAC/ISAO is fee-based. Industry has advised that they do not think that they should have to pay for TLP-Red or TLP-Amber information. The dissemination to industry needs to provide actionable intelligence quickly.
- Looking at other critical infrastructure industries, they have solved this issue by having a ISAC that worked closely with the regulators and sharing of information is prevalent as the ISAC scrubs all identifiable information. This moves the information out of the public domain and FOIA requests. A great example is FERC, NERC and the E-ISAC. Electric companies freely share this information as it cannot be made public. Sharing information directly with the USCG will make it FOIA susceptible.
- Especially in the convergence of the maritime and oil & gas industries, there are so many agencies and trade groups it is hard to notify everyone. So many notifications will eventually lead to leaks of business sensitive data. Example, do they notify the IT-ISAC, Maritime ISAC, ONG-ISAC, Maritime Transportation System ISAC, National Response Center, USCG, COTP, AMSC, FSO Groups, etc. A cyber event can easily impact most or all of these. Industry needs a streamlined notification system.
- Industry may perceive responsibilities under 33CFR 101.305 and CG-5P Policy Letter No. 08-16 as most important. These reporting requirements may not include a horizontal sharing component across industry. An issue is whether information-sharing should be limited to areas within direct USCG jurisdiction or broader enterprise security risks that may not rise to these reportable criteria. This could color the extent of information-sharing recommendations.
- There is a tremendous amount of Cyber Information coming from a wide variety of sources; industry may not know where to go for information.
- Industry may be concerned that, during the information exchange, they are subject to regulatory repercussions by the reporting process.
- **MTS-ISAC was purpose built to address these inefficiencies and gaps.**

- Outside of CISA's recent heightened efforts to share known exploited vulnerability information, there has been a lack of Federal sharing of actionable cyber threat information for the last 15 years
    - Information is shared weeks, months, and sometimes years later
    - Information is often generic in nature and critical infrastructure often struggles with knowing what to do with that information
    - Shift in CISA strategy to Joint Cyber Defense Collaborative excludes many critical infrastructure sectors, including Transportation
- Lack of government resources focused on declassification authorities
    - The goal should be to get critical infrastructure stakeholders the information they need to protect themselves and act against the threats targeting them
- Trying to use other Federal efforts that were purpose built to address different needs to address information sharing efforts
    - Area Maritime Security Committees, InfraGard Chapters, etc. were fundamentally created to address other needs and thereby are inefficient means to share information

- **MPS-ISAO Request for Information**

Findings from US DHS/CISA Cyber Storm VIII Exercise (March 2022) Included in Response Along with Other IACI, MPS-ISAO Information Sharing & Response Issues & Challenges

- **Issue:** Information sharing is siloed – limited sector sharing and no structured cross-sector sharing.
    - **Actionable Mitigation**: USCG, DHS, and private-sector cross-sector partners need to be identified, and included in info sharing, analysis and response structure. The IACI-CERT has implemented the global information sharing infrastructure – connecting MTS and other sectors for multi-directional information sharing, analysis and response.
- **Issue:** Lack of Security Convergence – Physical, Cyber-Physical, Cyber, Cognitive (Disinformation, Misinformation, Malign Influence) information sharing and response siloed.
    - **Actionable Mitigation:** MPS-ISAO and IACI leading development, training and certification of MTS Cyber First Responders – including alignment of physical, cyber-physical, cyber and cognitive response protocols – public/private collaboration.
- **Issue: Confusion – What to share, with whom to share, why to share, how to share, as well as architectures, methods and mechanisms of sharing.**
    - **Actionable Mitigation:** Need to connect-the-dots within MTS and across other critical infrastructure sectors including dependencies and interdependencies among and between sectors. Information sharing should not be seen as competition between ISAOs/ISACs or security companies. All need to contribute to the Common Operational Picture in order to respond effectively to treats and attacks.
- **Issue:** Need more coordinated USCG threat intel information sharing including accelerating and advancing MTS private sector and USCG cooperation, coordination and collaboration to address cyber threats and attacks.
    - **Actionable Mitigation:** The MPS-ISAO and IACI are addressing with the MTS Cyber First Responder Program (training/certification) that will include MTS-specific cyber info sharing, analysis, response coordination – connecting the dots….NOT DUPLICATING EFFORTS.
- **Issue:** Lack of information sharing reporting templates, what information is needed to be shared. Lack of development of a common operational picture for relevant information shared by one organization. Need to coordinate the structured collection and intake of information from multiple sources. Need to safeguard sensitive and classified information – protecting privacy.

        - **Actionable Mitigation:** Need to develop standards for the above – (USCG-led).
    - **Issue** – Ensure the right people receive the right intel at the right time. Ensure intel shared is "actionable" – NO INTEL FIREHOSE.
        - **Actionable Mitigation:** Requires coordination with the MTS sector to ensure intel info sharing requirements are being met. Need intel info sharing working group which the MPS-ISAO and IACI can help lead with USCG.
    - **Issue** – Lack of cybersecurity threat and defensive measures information sharing and response workforce education – based on MTS roles and responsibilities – need workforce skills development.
        - **Actionable Mitigation: Develop** MTS role-based cybersecurity education that communicates information sharing, analysis and response lifecycle, potential impacts, and individual workforce roles and responsibilities.

B. Identify real or perceived obstacles to cyber information sharing from MTS stakeholders to the government and from the government to MTS Stakeholders.

- It would be a good idea to leverage the local Sector in information-sharing. The Sector knows their facilities. There was a recommendation that we work with the Sectors and the AMSCs.
- Approaching the AMSC's through the Coast Guard contact, which may be the sole route to approach the AMSC, may not result in reaching the AMSC. There is a big diversity among the AMSCs, concerning industry participation and Coast Guard management styles. Due to the varied abilities and participation of the AMSCs around the country the NMSAC feels they should gather and share information where it is practicable but should not be relied on as an overall answer.
- There is a lack of horizontal information sharing among the AMSCs. If there is a conversation ongoing among the AMSC chairs, it is not being shared to the AMSC members.
- The Coast Guard has suspended national meetings of the AMSCs, with the exception of cyber subcommittee chairs. These meetings are not really sharing anything you cannot find in the public domain.
- There is uncertainty regarding the role of the fusion centers, which may need to be defined.
- Where does CISA figure into the equation?
- Most companies are hesitant to provide information on attacks, intrusions, or possible weaknesses to their networks with parties outside their organization without NDA's. The one exception we have seen is sharing with the FBI when law enforcement is needed to recover stolen assets.
    - Especially in the convergence of the maritime and oil & gas industries, there are so many agencies and trade groups it is hard to notify everyone. So many notifications will eventually lead to leaks of business sensitive data. Example, do they notify the IT-ISAC, Maritime ISAC, ONG-ISAC, Maritime Transportation System ISAC, National Response Center, USCG, COTP, AMSC, FSO Groups, etc. A cyber event can easily impact most or all of these. Industry needs a streamlined notification system.
- The IT organization usually works in a silo, not sharing information with the rest of the organization. They often are not integrated and have little sharing of threats or attacks with the physical security group unless it had a direct impact on a physical security system. Cyber threats and attacks are seen as top secret within an organization. If the IT group does not know of the NVIC or need to share this information with the above mentioned organizations, they will continue to not pass the information along.
- Information sharing in industry often times needs to be approved by multiple departments such as Corporate Communications and Legal. This adds time to any sharing or may even squash it.
    -
-
- **MTS-ISAC developed ways to overcome each of these obstacles.**

- From MTS to Government
  - Real: Government support of ISACs to gain access to more information
  - Perceived: Private sector doesn't share information with the government
- From Government to MTS
  - Real: Local and State governments outperforming Federal government in sharing cyber threat information
  - Perceived: Government isn't allowed to share because of concerns related to security information and classification concerns
  - Perceived: Government must lead information sharing efforts

- **MPS-ISAO Request for Information**

Findings from US DHS/CISA Cyber Storm VIII Exercise (March 2022) Included in Response Along with Other IACI, MPS-ISAO Information Sharing & Response Issues & Challenges

- **Issue** - Confusing federal government information sharing structure/contacts – who to contact for response and support? Lack of 'National Cyber Incident Response Plan (NCIRP)' designated public sector contacts.
  - **Actionable Mitigation**: Need to operationalize the NCIRP – within and across sectors. Not just a plan, an operationalized infrastructure, NCIRP contacts and collection sources.
- **Issue** – Lack of analyst resources to address actionable intelligence information sharing and response–what to do? Private-sector needs guidance and support.
  - **Actionable Mitigation**: Develop a surge capacity plan to provide analysis and response support during attacks and incidents.
- **Issue** – Lack of mass communication to the private sector regarding information sharing guidance, regulations, protections, process, what to share – who, what, when, why and how?
  - **Actionable Mitigation:** Need for mass MTS socialization of threat and defensive measures information sharing, analysis, and response resources.
- **Issue** – Lack of secure communications. Variety/excess of communication channels.
  - **Actionable Mitigation:** The IACI-CERT and the MPS-ISAO are providing the MTS sector with military-grade encrypted communications (chat, direct messaging, file sharing, response coordination). Need to connect the MTS sector (public and private) with response protocols.
- **Issue** – Information Sharing and Response Trust issue from the private-sector to government,
  - **Actionable Mitigation:** Need to communicate the Cybersecurity Information Sharing Act of 2015 that gives critical infrastructure owners and operators information sharing protections. Too many have never heard of it.

C. Provide actionable short-term and long-term recommendations for enhancing cyber information sharing between the government and MTS stakeholders that take into consideration the existing information sharing framework.

Although Coast Guard has many initiatives underway to help the Marine Transportation System (MTS) they are just that and are underway. The time to act is now, the MTS cannot wait any longer to share information bilaterally.

- Recommend that we pursue working with the MSP-ISAO and MTS-ISAC where practicable to increase cyber information-sharing. A value in engaging both is the ability for the anonymization of information for broader distribution. This may alleviate concerns about reporting to the USCG.

    - The Maritime and Port Security Information Sharing and Analysis Organization (MPS-ISAO) was formed in 2016 as a public- and private-sector collaborative partnership advancing security resilience.
        - Among other services, the organization makes available Threat Intelligence Reports and Advisories (TLP-Green) to "vetted" Maritime & Port critical infrastructure stakeholders.
        - The organization represented the maritime sector in the 2020 CISA exercise Cyberstorm
        - The organization emphasizes eliminating barriers and silos between cyber stakeholders
- The Maritime Transportation System Information Sharing and Analysis Center (MTS-ISAC) promotes and facilitates maritime cybersecurity information sharing, awareness, training, and collaboration efforts between private and public sector stakeholders.
        - Among other services, provides proactive cyber threat intelligence, alerts, warnings, and vulnerability information cultivated from maritime stakeholders and public and private sector shares, open-source intelligence and cybersecurity news.
        - The organization identifies their Cyware product, their emphasis on peer-to-peer connections, and their thought leadership as important contributions to cybersecurity information sharing
- Recommend that Coast Guard resume national meeting of AMSCs (in the past, these were combined Harbor Safety Committee/AMSC meetings) focusing on all hazards, not just cyber
- Recommend that CG-CYBER or CG-FAC dedicate a page on their websites to cyber information sharing, details on content to be a further NMSAC tasking.
- Recommend the Coast Guard determine exactly what type of cyber threat information they want to receive and are willing to coordinate the sharing of, preferably at no cost to stakeholders. Are the limitations tied to anything that constitutes suspicious activity, a BoS, or a TSI under MTSA or will it include broader cyber threat and event reporting that has application to MTS enterprise security beyond MTSA requirements? This determination is important for two reasons:
    - Without defining reporting criteria (required or recommended) that is either limited to MTSA-related reporting or expanded to enterprise level reporting, there will be confusion regarding how extensive the USCG access to cyber intel is. In other words, there may be an assumption that the USCG is the clearinghouse for all MTS cyber intelligence when in fact its only MTSA related reporting. Facilities have large numbers of systems, whose compromise may not fit neatly into a reportable event.
    - Some elements of the MTS are concerned about cyber threats to adjacent transportation systems (ie. Trucking and rail) as well as business systems that USCG may not have responsibility over. Would there be an expectation that USCG would coordinate with other US government entities on these touch points or is it up the facilities?
- There is a significant difference in the MTS' efforts to manage enterprise security risk (ie. Risk to their operations, profitability, and viability) and managing regulatory compliance.
- Encourage industry to include IT into the trade groups and security organizations such as AMSC and FSO groups. Add content that is IT specific into the meetings to encourage the company teams to work together.
- Educate both government and industry partners on the convergence of physical and cyber security attacks and threats. Talk about attacks that coordinated cyber and physical attacks into one. One example is the PG&E attack in San Jose.
- Form a working committee to meet with other ISAC's to see how they are tackling this issue and bring the best of breed ideas back for consideration.
- **MTS-ISAC developed ways to overcome each of these obstacles.**
    - Short-term
        - USCG CPT provides anonymized periodic reports related to commonly seen findings
        - USCG supports MTS-ISAC delivery of threat information to all regulated facilities
        - Establish baseline understanding of current threat activity

        - Bridge the gap between the strategic role of AMSC Cybersecurity Subcommittees and need for actionable, threat information
        - USCG joins Federal, State, and local governments in having a representative to the MTS-ISAC
    - Long-term
        - USCG partners with public and private sector stakeholders to enact information sharing strategies, operational activities, and tactical engagement to further improve the preparedness and response capabilities of the community
- **USCG Intelligence (CG-2)**
    - Long Term Goal:

The Coast Guard Intelligence (CG-2) "Threat Intelligence Partnership for MTS Cybersecurity" prototype would be considered a Long-Term goal of CG-2. This would provide more coordinated USCG threat intel information sharing including accelerating and advancing MTS private sector and USCG cooperation, coordination, and collaboration to address cyber threats and attacks. It is currently in the Level of Effort –1 (LOE-1). This would be a voluntary program at no cost for the MTS and the sharing of actionable intelligence would be shared with the downstream consumers such as the MTS, the MTS-ISAC, MPS-ISAO, Maritime ISAC, Cybersecurity, and Infrastructure Agency (CISA), Federal Bureau of Investigation (FBI), Maritime Exchange for Data Security (MEDS) and many others.

Currently, the prototype is ingesting cyber threat data from the MPS-ISAO, Louisiana State and Analytical Fusion Center (LA-SAFE) and CISA as it continues to develop.

X. APPROVAL AND AUTHORITY TO SUBMIT TO USCG

The Sub-Committee approves this report to be submitted to the full NMSAC for approval to submit to USCG.

Name	Title	Date
Laurie Thomas	Chair	
Ed Madura	Co-Chair	

Approved By	Date	Approved By	Date